

AMENDMENTS TO THE CLAIMS

The following listing of claims will replace all prior versions, and listings, of claims in this application:

1 1. (Currently Amended) A method for generating a cryptographic key using at
2 least one parameter comprising the steps of:
3 generating at least one index as a function of said at least one parameter, said one
4 parameter being from a plurality of varying parameters;
5 retrieving at least one cryptographic share from a memory location identified as a
6 function of said at least one parameter~~index~~; and
7 generating a cryptographic key based on said at least one cryptographic share.

1 2. (Original) The method of claim 1 wherein said at least one retrieved
2 cryptographic share is encrypted, said method further comprising the step of:
3 decrypting said at least one cryptographic share.

21
1 3. (Original) The method of claim 2 wherein said step of decrypting comprises
2 the step of:
3 decrypting using a value computed as a function of said at least one parameter.

1 4. (Original) The method of claim 1 wherein said at least one retrieved
2 cryptographic share is compressed, said method further comprising the step of:
3 decompressing said at least one cryptographic share.

1 5. (Currently Amended) The method of claim 4 wherein said step of
2 decompressing comprises the step of:
3 decompressing said at least one cryptographic share using ~~an~~ said ~~index of~~ to said
4 memory location.

1 6. (Original) The method of claim 1 wherein said at least one parameter
2 represents at least one measurement of a physical property.

1 7. (Currently Amended) The method of claim 1 ~~further comprising the step~~
2 ~~of wherein the plurality of varying parameters change from one said generation of said~~
3 ~~cryptographic key to a next generation of said cryptographic key.~~
4 ~~generating at least one index as a function of said at least one parameter; and~~
5 ~~using said index to identify said memory location.~~

1 8. (Original) The method of claim 7 further comprising the step of:
2 retrieving a cryptographic share from a memory location in the vicinity of said
3 memory location identified by said index.

1 9. (Original) The method of claim 7 wherein said step of generating at least one
2 index comprises the step of generating the same index for a set of parameter values.

1 10. (Original) The method of claim 9 wherein said set of parameter values are
2 within a predetermined range of values.

1 11. (Cancelled)

1 12. (Cancelled)

1 13. (Cancelled)

1 14. (Cancelled)

1 15. (Cancelled)

1 16. (Cancelled)

1 17. (Cancelled)

1 18. (Cancelled)

1 19. (Cancelled)

1 20. (Cancelled)

1 21. (Cancelled)

1 22. (Cancelled)

1 23. (Cancelled)

a1
1 24. (Currently Amended) A method for generating a cryptographic key
2 comprising the steps of:
3 measuring a plurality of keystroke features during entry of a password;
4 generating a plurality of indices using said plurality of keystroke features;
5 retrieving from a data structure a plurality of cryptographic shares as a function of
6 ~~said plurality of keystroke features~~said plurality of indices; and
7 generating a cryptographic key using said cryptographic shares.

1 25. (Original) The method of claim 24 wherein said cryptographic shares
2 represent points on a polynomial.

1 26. (Original) The method of claim 24 wherein said cryptographic shares
2 represent vectors.

1 27. (Original) The method of claim 24 wherein said cryptographic shares are
2 compressed.

28. (Original) The method of claim 27 wherein said cryptographic shares comprise y values of points on a polynomial and the corresponding x values are derivable from a data structure location.

29. (Currently Amended) The method of claim 24 ~~further comprising the step of:~~ wherein said plurality of keystroke features vary from said generating of said cryptographic key to a next generation of said cryptographic key generating a plurality of indices as a function of said keystroke features; and using said plurality of indices to identify locations within said data structure from which to retrieve said cryptographic shares.

30. (Currently Amended) The method of claim ~~29-24~~ wherein said step of generating a plurality of indices as a function of said keystroke features comprises the step of:

for each of said keystroke features, generating one of two indices as a function of a threshold value, h_i , where said function is defined by:

$$f(\phi_1, \phi_2, \dots, \phi_m) = \{\psi_1, \psi_2, \dots, \psi_m\} \in \{0, 1\}^m$$

where

ϕ represents said keystroke features, ψ represents said indices, m is a particular number of measured features associated with said password; and

$$\psi_i = \begin{cases} 0 & \text{if } \phi_i < h_i \\ 1 & \text{if } \phi_i \geq h_i \end{cases}$$

31. (Currently Amended) The method of claim ~~29-24~~ wherein said step of generating a plurality of indices as a function of said keystroke features comprises the step of:

for each of said keystroke features, generating one of a plurality of indices as a function of a plurality of threshold values, h_i , where said function is defined by:

$$f(\phi_1, \phi_2, \dots, \phi_m) = \{\psi_1, \psi_2, \dots, \psi_m\} \in \{0, 1\}^m$$

where

ϕ represents said keystroke features, ψ represents said indices, m is a particular number of measured features associated with said password; and

$$\psi_i = \begin{cases} 0 & \text{if } \phi_i < h_i \\ 1 & \text{if } \phi_i \geq h_i \end{cases}$$

32. (Original) The method of claim 24 wherein said cryptographic shares stored in said data structure are encrypted, said method further comprising the step of: decrypting said cryptographic shares using said password.

33. (Original) The method of claim 24 further comprising the steps of: maintaining a history file containing information relating to prior successful key generation attempts; and based on said history file, storing invalid cryptographic shares in data structure locations which are not expected to be accessed during subsequent legitimate key generation attempts.

34. (Currently Amended) A method for generating a cryptographic key using a plurality of varying parameters, said having a sequence and varying parameters representing physical measurements, said method comprising the steps of:

for each of said plurality of parameters:

generating at least one index using said parameter;

retrieving an encrypted cryptographic share from a memory location as a function of ~~the sequence of said parameters~~ said at least one index;

decrypting said encrypted cryptographic share with a function of said parameter; and

generating a cryptographic key using said decrypted cryptographic shares.

1 35. (Original) The method of claim 34 wherein said physical measurements are
2 measurements of DNA.

1 36. (Original) The method of claim 34 wherein said function of said parameter
2 used to decrypt said encrypted cryptographic share is a hash function.

1 37. (Currently Amended) A data structure for use in generating a cryptographic
2 key based on n parameters representing physical measurements, said data structure
3 comprising:

a1 4 n storage locations each associated with a respective one of said n parameters,
5 each particular storage location containing an encrypted cryptographic share which was
6 encrypted using an expected value of a function of the parameter associated with said
7 particular storage location, each said n storage location being associated with at least one
8 index of a plurality of indices, where said plurality of indices are generated using said
9 physical measurements.

1 38. (Original) The data structure of claim 37 wherein said function is a hash
2 function.

1 39. (Original) The data structure of claim 37 wherein said cryptographic key may
2 be generated using less than n cryptographic shares.
